

## REMARKS

Applicants appreciate the thorough review of the present application as reflected in the Official Action mailed December 15, 2004. Applicants also appreciate the withdrawal of the previous rejections. Applicants have amended Claims 37, 40 and 42 to correct a typographic error with regard to the secret value that is replaced with the key value.

### The IDS

Applicants wish to bring to the attention of the Examiner an Information Disclosure Statement that was filed with Applicants' previous response. Applicants note that the IDS appears in PAIR as filed July 2, 2004. Applicants request that the Examiner consider the materials cited in the IDS and return an initialled copy of the PTO-1449 form with any subsequent communication.

### The Obviousness Rejections

Claims 2-16, 18-34 and 36-42 stand rejected under 35 U.S.C. § 103 as obvious in light of the combination of United States Patent No. 5,337,357 to Chou *et al.* (hereinafter "Chou") and United States Patent No. 6,408,390 to Saito (hereinafter "Saito"). Official Action, p. 2.

#### *Claims 2, 15, 39 and 41*

Claims 2, 15, 39 and 41 are independent claims. In rejecting Claims 2, 15, 39 and 41, the Official Action acknowledges that Chou does not disclose generating a second key from the first key value and the first secret key value, encrypting the decrypted portion of the software with the second key value and storing the portion of the software encrypted with the second key value. Official Action, p. 3. The Official Action, however, relies on Saito, col. 13, lines 44-53, col. 24, line 46 to col. 25, line 5 and col. 14, lines 17-34 as teaching these recitations. Official Action, pp. 3-4.

Applicants submit that one of skill in the art would not be motivated to combine Chou and Saito in the manner recited in the claims. Chou encrypts the software with a key (K) and then obtains a first key value ( $K_1$ ) from a user. Chou, Figure and col. 3, lines 48-58. Based on the key K used to encrypt the software, Chou

determines a second key ( $K_2$ ) that, when combined with the first key  $K_1$ , results in the key K used to encrypt the software. Chou, Figure and col. 4, lines 7-11. Thus, if the key used to encrypt the software is changed, the system of Chou would be unable to generate the second key value to provide to a user as the processing center would not know what key was used to encrypt the software.

The way Chou prevents further subsequent installations on different computers is through a unique random factor, such as the use of a time dependent unique factor. *See* Chou, col. 2, line 57 to col. 3, line 13. The cited portions of Saito, in contrast, generate a new key that is used to encrypt the decrypted data. *See* Saito, col. 24, line 65 to col. 25, line 15. It does not appear that the system of Chou would work when combined with the cited portions of Saito because Chou relies on the software being encrypted with the key K. If the software were encrypted with a new encryption key, the system of Chou would not know how to create the two keys that, when combined, would result in the new encryption key. Thus, it appears that Chou relies on the software always being encrypted with the same key K so that it can calculate a  $K_2$  that, when combined with the key  $K_1$  provided by the user, may generate K. As such, Applicants submit that one of skill in the art would not be motivated to combine Chou and Saito as doing so would appear to eliminate the mechanism in Chou for controlling software installation.

In light of the above discussion, Applicants submit that Claims 2, 15, 26, 39 and 41 and the claims that depend from them are patentable over the cited references fro at least these reasons. Accordingly, allowance of these claims is respectfully requested.

*Claims 26, 37, 40 and 42*

Independent Claim 26 recites, in part:

generating the first key value from the obtained second secret value and the first secret value;

decrypting the first encrypted portion of the software utilizing the first key value;

generating the first key value based on the first and second secret values at the network server; and

associating the first key value with the identification of the copy of the software as an updated second secret value to be provided in response to a subsequent request for the second secret value.

Thus, Claim 26 recites that the first key value (the value used to decrypt the encrypted portion of the software) is used as one of the secret values that is used to generate a subsequent first key value. Independent Claim 37 similarly recites, in part:

generating a first key value from the first and second secret values associated with the copy of the software; and  
style="padding-left: 40px;">associating the first key value with the software identification of the copy of the software as an updated second secret value.

Claims 40 and 42 incorporate means-plus-function recitations and computer program code recitations, respectively, corresponding to the method recitations of Claim 37.

The same portions of Chou and Saito discussed above are cited in rejecting Claims 2, 15, 39 and 41 are cited in rejecting Claims 26, 37, 40 and 42. Applicants, however, fail to see in the cited portions of Chou and Saito where the use of a first key as one of two secret values for subsequent generation of a key as recited in these claims is found. Applicants do note that a third key Ks3 does appear to be described in various portions of Saito (e.g., col. 29, lines 28-34) but, based on a search for the term Ks3 in Saito, it does not appear to be generated based on two secret values where one is the previous encryption key but only states that the third secret key may be generated based on the second secret key. See Saito, col. 29, lines 28-31. As discussed above, Chou relies on the encryption key not changing. While the cited portion of Saito does describe generating a key from the encryption key, there is no indication that subsequent encryption keys are generated from the generated key. In fact, the particular language of Claims 26, 37, 40 and 42 does not appear to be discussed in the Official Action.

In light of the above discussion, Applicants submit that Claims 26, 37, 40 and 42 are not disclosed or suggested by the cited portions of Chou and Saito. Applicants also submit that the claims that depend from Claims 26 and 37 are patentable at least as depending from a patentable base claim.

*Claim 34*

Independent Claim 34 recites, in part:

wherein the step of decrypting the first encrypted portion of the software comprises decrypting an encrypted block of the plurality of encrypted blocks with the first key value;

wherein the step of encrypting the decrypted first encrypted portion of the software comprises encrypting the decrypted block with the second key value;

wherein the step of storing the first encrypted portion of the software encrypted with the second key value comprises storing the block encrypted with the second key value; and

wherein the block of the plurality of encrypted blocks is decrypted, encrypted and stored before a next block of the plurality of blocks is decrypted, encrypted and stored.

Thus, Claim 34 recites that the encrypted portion is broken into blocks and a block is decrypted, encrypted and stored before a next block is decrypted, encrypted and stored. Applicants fail to see where these recitations are addressed in the Official Action. Applicants submit that the cited portions of Chou and Saito do not describe such blockwise operations. Accordingly, Applicants submit that Claim 34 is patentable over the cited references for at least these reasons.

#### *The Dependent Claims*

Applicants submit that the dependent claims are patentable at least as depending from a patentable base claim. Applicants also submit that many of the dependent claims are separately patentable. For example, Claim 9 recites "the installation client is further configured to sequentially decrypt ones of the plurality of encrypted blocks with the first key value and sequentially encrypt and store the decrypted plurality of encrypted blocks with the second key value, wherein a next of the plurality of encrypted blocks is decrypted after a previous of the plurality of encrypted blocks is encrypted with the second key value and stored." In rejecting Claim 9, the Official Action cites to col. 14, lines 17-34 of Saito. Official Action, p. 4. However, this portion of Saito does not describe such a sequential process as recited in Claim 9. Accordingly, Applicants submit that Claim 9 is separately patentable over the cited references for at least these additional reasons.

In re: Matyas, Jr., et al.  
Serial No.: 09/642,685  
Filed: August 21, 2000  
Page 19 of 19

**Conclusion**

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,



\_\_\_\_\_  
Timothy J. O'Sullivan  
Registration No. 35,632

USPTO Customer No. 20792  
Myers Bigel Sibley & Sajovec  
Post Office Box 37428  
Raleigh, North Carolina 27627  
Telephone: 919/854-1400  
Facsimile: 919/854-1401